APAFAM

Formación Dirigida en FM

**Desarrollado en el marco de la celebración del**

WORLDFMDAY

Haciendo Una Verdadera Diferencia

10 MAY 2023

A Global FM™ initiative

APAFAM

Formación Dirigida en FM

# GESTION DE RIESGOS DE SEGURIDAD

INSTRUCTOR:

**ING. ALFONSO ALIZO, ProFM**

04 DE ABRIL DE 2023

# OBJETIVOS

- Describir los principios, el marco y el proceso de gestión de riesgos,
- Identificar el enfoque de la Gestión de Riesgos de Seguridad
- Identificar que abarca la seguridad física y como se estructura el servicio.
- Identificar la importancia de la seguridad cibernética en las instalaciones actuales.
- Reconocer la importancia de la gestion de riesgo en la elaboración de un Plan de Emergencia.
- Reconocer el alcance del FM en la elaboración del Business Continuity Plan (BCP) – Plan de Continuidad de negocios.

# GESTIÓN DE RIESGOS

Podemos decir que el riesgo es algo desconocido que, si se produce, afecta en forma negativa o positiva (una actividad, un mantenimiento, un proyecto). Por lo tanto, un evento incierto puede ser algo bueno (oportunidad) o algo malo (amenaza)

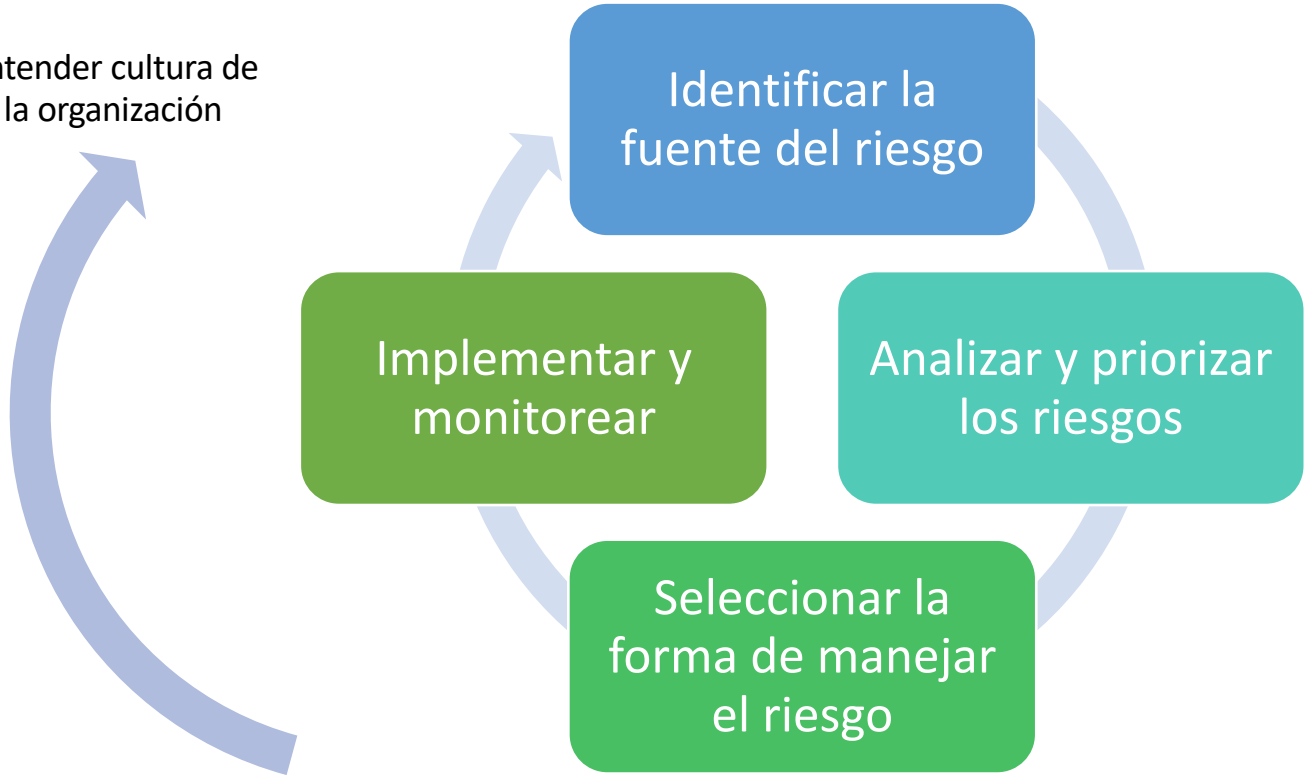
**Riesgo**= **P** (probabilidad) x **S** (severidad)


La gestión de riesgos se puede definir como el proceso de identificación, análisis y tratamiento de los problemas a los que se enfrenta una organización.


La gestión exitosa de los riesgos de significa estar preparado y estar vigilante. Se analizan los datos de amenazas para identificar y priorizar los desafíos de seguridad.

# GESTIÓN DE RIESGOS

Entender cultura de la organización




# PLANIFICACIÓN DE GESTIÓN DE RIESGOS

- ¿Quiénes van a identificar los riesgos?
- ¿Cuándo se llevará a cabo la identificación de los riesgos?
- ¿Qué escala se utilizará para el análisis cualitativo de riesgos?
- ¿Cómo se priorizarán los riesgos?
- ¿Qué herramientas se utilizarán para el análisis cuantitativo?
- ¿Cuáles serán las estrategias a implementar para cada riesgo?
- ¿Con qué frecuencia se realizará el monitoreo de riesgos?

# MATRIZ DE RESPUESTA AL RIESGO

Impacto

Probabilidad

| | Muy Bajo (1) | Bajo (2) | Moderado (3) | Alto (5) | Muy Alto (10) |
|---|---|---|---|---|---|
| Muy baja (1) | Aceptar | Aceptar | Aceptar | Aceptar | Transferir /Mitigar |
| Baja (2) | Aceptar | Aceptar | Aceptar | Transferir /Mitigar | Evitar |
| Moderada (3) | Aceptar | Aceptar | Aceptar | Transferir /Mitigar | Evitar |
| Alta (4) | Aceptar | Aceptar | Transferir /Mitigar | Evitar | Evitar |
| Muy alta (5) | Aceptar | Transferir /Mitigar | Transferir /Mitigar | Evitar | Evitar |

## ESTRATEGIAS DE RESPUESTA A CONTINGENCIAS:

- Definir **señales de advertencia** y diseñar acciones (planes de reserva o contingencias) que se implementarán en caso de contingencias.
- Incluir siempre un **dueño del riesgo** (custodio o propietario) en cada acción que se decida implementar como respuesta al riesgo.

# ESTRATEGIAS PARA AMENZAS

**ESCALAR**

Cuando el riesgo está fuera de los límites de la autoridad del FM, trasladar la decisión sobre la respuesta del riesgo a un nivel superior. Se debe mencionar explícitamente quién será notificado sobre ese riesgo.

**EVITAR**

Cambiar las condiciones originales de realización de la actividad (proyecto, mantenimiento) para eliminar la probabilidad de ocurrencia del riesgo identificado. (si una tecnología importada originará problemas, evitar sería reemplazar esa tecnología por otra).

**TRANSFERIR**

Trasladar el impacto negativo del riesgo hacia un tercero (contratar un seguro o colocar una penalidad en el contrato con el proveedor).

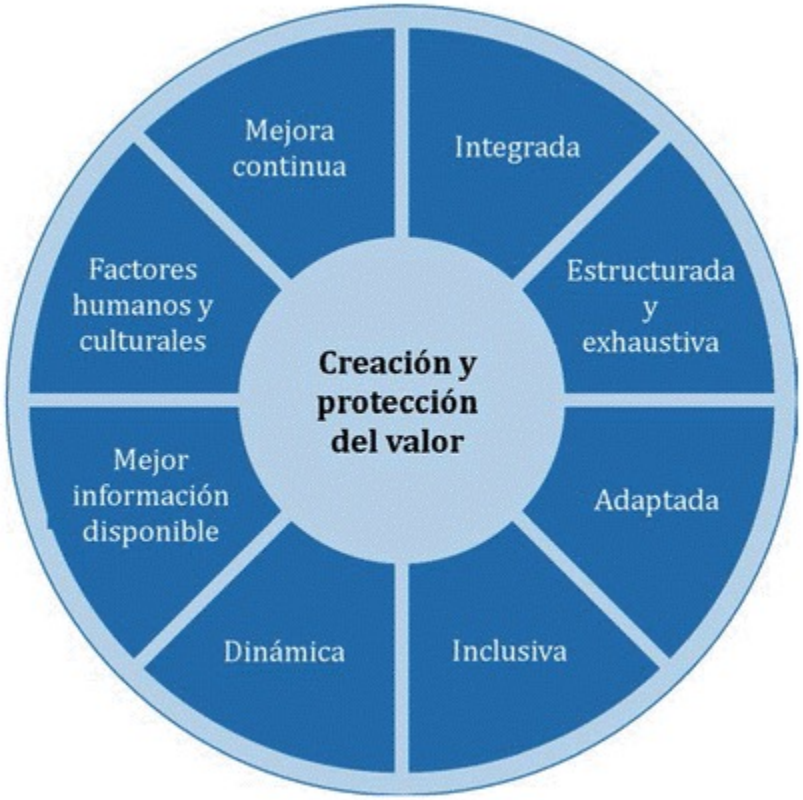
**MITIGAR**

Disminuir la probabilidad de ocurrencia y/o el impacto. (instalar un sistema de alarmas en caso de incendio).

**ACEPTAR**

No cambiar probabilidad o impacto. En la aceptación activa se define cómo actuar en caso que ocurra el riesgo. Por ejemplo, instrucciones de cómo seguir facturando si hay un corte de energía o establecer una reserva para contingencias. En una aceptación pasiva, no se planifican acciones o reservas con anticipación, sino que se actúa sobre el riesgo una vez que aparece.

# GESTIÓN DE RIESGO ISO 31000. PRINCIPIOS

# COSTOS ASOCIADOS A UNA INEFICIENTE GESTIÓN DE RIESGOS

- Costo Financiero.
- Pérdida de capital humano.
- Perdida de reputation.

# ALCANCE DE LA GESTION DE RIESGOS DE SEGURIDAD

- Seguridad de los ocupantes, visitantes y personal.
- Seguridad de los activos de las instalaciones.
- Protección de la información de la organización.

# SEGURIDAD FÍSICA

El objetivo es mitigar (disminuir la amenaza), bloquear cualquier amenaza nueva y reducir las consecuencias si no se puede prevenir la amenaza

- Evaluar los riesgos de seguridad.
- Desarrollar un plan de mitigación.
- Implementar los cambios necesarios en la instalación y los procesos.
- Asumir la responsabilidad de la seguridad de los sistemas FM.

## ENFOQUES DE MITIGACIÓN DE LA SEGURIDAD FÍSICA

- Sistemas de CCTV.
- Control de Acceso.
- Barreras Perimetrales.
- Sistema de Alarma.
- Etiquetado de propiedades.
- Equipo de Seguridad.
- Procesos de Acceso.

El objetivo

de la mitigación es disminuir la amenaza, bloquear cualquier amenaza nueva y reducir las consecuencias si no se puede prevenir la amenaza

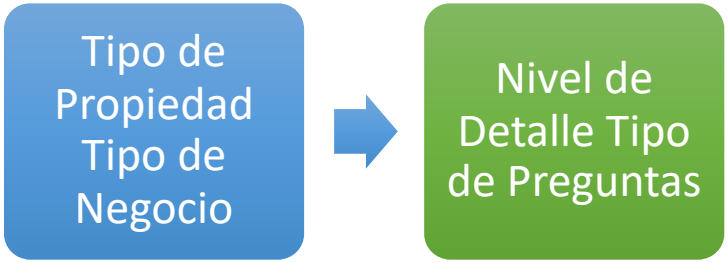
# SEGURIDAD FÍSICA

Es la protección de datos, equipos, ocupantes, visitantes, sistemas y otros activos de la organización.

- Las amenazas físicas incluyen:
- Acceso no autorizado.
- Acciones agresivas.
- Sabotaje.
- Daño.
- Robo.

# ALCANCE DE LA SEGURIDAD

**Auditoría Integral de Seguridad de las instalaciones :** Identificar qué tan bien está protegida la instalación contra amenazas físicas probables


Proceso de revisión y mejora continua, los planes pierden su efectividad con el tiempo si no son monitoreados.

# LISTA DE VERIFICACIÓN DE SEGURIDAD DE LAS INSTALACIONES

| SI/NO | RIESGO |
|---|---|
| | ¿Se cuenta con un procedimiento para el control de llaves o tarjetas de acceso? |
| | ¿Se inspecciona la basura antes de salir de la instalación? |
| | ¿Inspecciona los paquetes y bolsas de los empleados antes de salir de las instalaciones? |
| | ¿Hay un registro completo de quien tiene que llaves o tarjetas de acceso? |
| | ¿Permite a los empleados retirar el equipo? ¿Qué equipos? |

# GESTIÓN DE RIESGOS DE LA VIOLENCIA EN EL LUGAR DE TRABAJO: POLÍTICAS

Crear políticas y procedimientos basados en:

- Amenaza de violencia → Comportamientos
- Violencia en el lugar de trabajo → Plan de respuesta

## POLÍTICA DE VIOLENCIA EN EL LUGAR DE TRABAJO

- Asegúrese de que sea breve y fácil de entender.
- Usa un lenguaje sencillo.
- Evite términos absolutos.
- Evite definiciones estrechas.
- Utilice la revisión por parte de legal.

# GESTIÓN DE RIESGOS DE LA VIOLENCIA EN EL LUGAR DE TRABAJO: PREVENCIÓN

## LA PROTECCIÓN FÍSICA INCLUYE

- Barreras físicas.
- Sistemas de alarma o botones de pánico.
- Cámaras de vigilancia/televisión de circuito cerrado.
- Personal de seguridad uniformado visible.
- Iluminación luminosa en los terrenos y en los estacionamientos.
- Vidrio a prueba de balas.
- Limitar el acceso del público a las instalaciones.
- Servicio de acompañantes fuera del horario laboral para los empleados.
- Detectores de metales en los puntos de entrada a la instalación.

La prevención se puede mejorar a través de cambios en la instalación física y en los procesos.

# GESTIÓN DE LOS EFECTOS DE LOS INCIDENTES

**REVISIÓN POSTERIOR**

- Lo que sucedió (paso a paso).
- Si la respuesta a la situación era apropiada.
- Resultado.
- Lecciones aprendidas.
- Detalles apropiados para compartir con los empleados y la familia de la víctima.

**ACCIONES DEL FM**

- Estar presente y disponible.
- Difundir la información correcta.
- Disipar los rumores.
- Alertar al equipo de gestión de crisis para dar respuesta profesional.
- Mantener conversaciones informales.
- Mantener juntos los grupos de trabajo y los equipos.
- Fomentar la conversación entre los miembros del equipo.
- Ayudar a los empleados a enfrentar los temores de lugares o personas.

# CIBERSEGURIDAD

Es la tecnología, las prácticas y los procesos utilizados para proteger las redes internas, los ordenadores y los programas de datos de una organización de un ataque.

*Seguridad operativa

*La información.

*La Red

*La seguridad de las aplicaciones.

*Continuidad del negocio/recuperación ante desastres.

Se pide continuamente a los FM que entreguen edificios "inteligentes", pero la entrega de ese nivel de tecnología crea vulnerabilidades y eficiencias operativas.

# INTEGRACIÓN DE SISTEMAS DE SEGURIDAD

Un edificio inteligente es aquel que utiliza la tecnología para crear un entorno más confortable, seguro y productivo para sus ocupantes y más eficiente operativamente para sus propietarios

- SISTEMAS CONECTADOS
- SENSORES POR TODAS PARTES
- AUTOMATIZACION

# NORMAS BÁSICAS DE CIBERSEGURIDAD

## CONFIDENCIALIDAD

- Privacidad.
- Controles sobre quién puede acceder a los datos.
- Limitaciones sobre quién puede modificar o eliminar datos.

## INTEGRIDAD

- Fiabilidad de los dato.
- Fiabilidad del almacenamiento de datos.
- Autenticidad de los resultados generados a partir de data.

## DISPONIBILIDAD

- Accesibilidad de los sistemas cuando sea necesario.
- Asociación con otras funciones empresariales.

# GESTION DE RIESGO CIBERNETICO

- Identificar el riesgo o la amenaza cibernética potencial.
- Analizar las amenazas potenciales, incluidos los tipos de amenazas y vulnerabilidades.
- Gestionar o mitigar el riesgo mediante el diseño de las medidas de seguridad adecuadas.
- Supervisar y controlar los impactos actuales y futuros del riesgo

# LISTA DE VERIFICACIÓN DE CIBERSEGURIDAD

| SI/NO | RIESGO |
|---|---|
| | ¿Se ha realizado una revisión de los tipos de datos que la organización ha almacenado en diferentes sistemas ? |
| | ¿Están cifrados los datos del sistema de la organización? |
| | ¿Existe una política de ciberseguridad? ¿Se ha capacitado a los empleados en ciberseguridad? |
| | ¿Los empleados y proveedores solo tienen acceso a los sistemas que necesitan? |
| | ¿Ha purgado la organización las cuentas “antiguas” del sistema o las ha cerrado? |
| | ¿Se realiza una copia de seguridad rutinaria de los datos del sistema? |
| | ¿Se actualizan de forma rutinaria el cortafuegos, el software antivirus y los parches de seguridad? |
| | ¿Se han cambiado todas las contraseñas predeterminadas en todos los dispositivos? |

# CIBERSEGURIDAD. POLÍTICAS Y CONTROLES

- Programas de Ciberseguridad (firewall, protección contra Malware).
- Control de Actualizaciones y Parches.
- Procedimientos de Copia de Seguridad y Recuperación de Datos.
- Uso permitido de Internet (incluido el acceso y uso de las redes sociales).
- Procedimientos para el acceso remoto a la red.
- Uso de dispositivos personales para conectarse a la red.
- Creación, Control y Mantenimiento de Contraseñas.

Al igual que cualquier otra política, la política de ciberseguridad debe ser revisada y mantenida regularmente.

# MANEJO DE EMERGENCIAS

- Una **emergencia** es cualquier evento causado por el hombre, por la tecnología o un evento natural que ponga en riesgo a las personas, a la propiedad, a la operación o el medio ambiente en una organización.
- **Manejo de Emergencias** hace referencia a la preparación que debe tener todo Departamento de Facility Management para atender situaciones adversas que puedan ocurrir y cómo recuperarse de ellas **(Gestión)**


**BENEFICIOS PARA EL FM y PARA LA ORGANIZACIÓN**

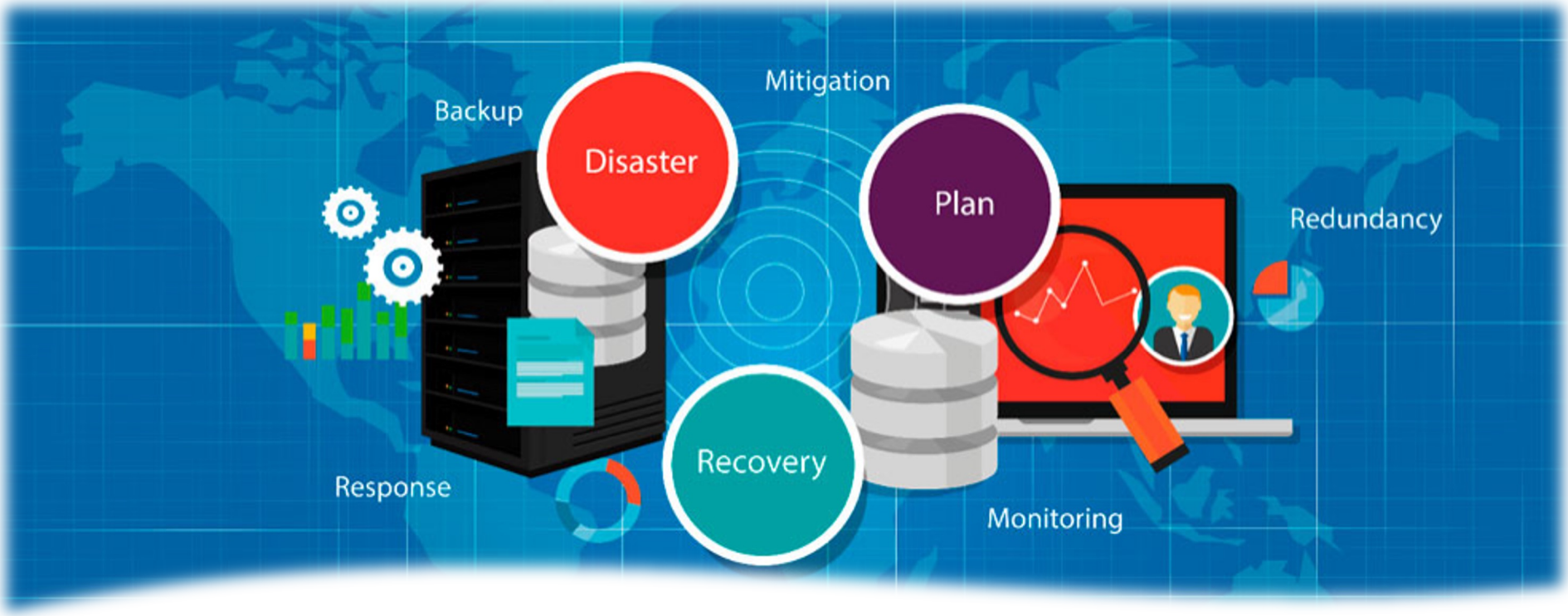
- **Reducir el Impacto de la emergencia**
- **Proteger y restaurar la operación (Core Business)**

# RETOS DE UN FM EN EL MANEJO DE EMERGENCIAS


# CONTINUIDAD DEL NEGOCIO

- ISO 22301 define **Continuidad del Negocio** como “la capacidad de una organización de continuar la entrega de productos o servicios a un nivel aceptable predefinido después ocurrido un incidente disruptivo.

- La mayoría de las organizaciones experimenta una interrupción mayor cada cuatro años.




# PLANEACIÓN DE LA CONTINUIDAD DEL NEGOCIO

1. Determine el alcance y asignación razonable de recursos para lograrlo
2. Ejecute un análisis de impacto y de riesgo del negocios
3. Cree la estrategia de continuidad del negocio
4. Establezca y ejecute los procedimientos de continuidad del negocio
5. Pruebe, comunique y entrene en estos procedimientos

# MANEJO DE EMERGENCIAS

## Análisis del Impacto en el Negocio

- Ayuda a la organización a entender, planear y mitigar vulnerabilidades
- Los tres recursos principales que debemos proteger son:
  - Personas
  - Propiedad
  - Registros Críticos

| Ejemplos de Registros Críticos |
| --- |
| • Perdida o Fallo de A/A.<br>• Fallo en servidores (no acceso a Red)<br>• Perdida de Información (corrupción de Disco Duro, Daño servidor, daño archivo)<br>• Inundación y/o ruptura de tubería<br>• Afectación de personas dentro de la propiedad (caída, tropiezos, lesiones)<br>• Correspondencia de la organización |

## Desarrollo del Plan de Contingencias

- Definir puntos y responsabilidades que activan el plan
- Definir un plan de sucesión de posiciones clave
- Proveer acceso continuo a los registros actuales del negocio
- Desarrollar estrategias de operación "qué pasa si"
- Establecer los medios para asegurar los niveles requeridos de personal
- Contratar la entrega de insumos necesarios, servicios tercerizados y provisión de sitios y equipos de contingencia

**RESPONSABILIDADES DEL FACILITY MANAGER DURANTE UN INCIDENTE:**

- Coordinar los recursos y esfuerzos de la organización.
- Ejecutar los planes de evacuación (según sea necesario).
- Liderar la porción de los esfuerzos de respuesta.
- Uso del plan de manejo de emergencia.
- Actuar como la primera respuesta de la organización.
- Aconsejar e informar a la alta gerencia.
- Proveer la seguridad de la propiedad y limitar acceso al sitio.
- Dirigir la respuesta de la organización.

# RESPUESTA A INCIDENTES

# PLAN DE MANEJO DE EMERGENCIA

## PLAN DE MANEJO DE EMERGENCIA

- Dirección/ubicación y procedimientos del Centro de Control de Emergencias de la organización
- Roles y responsabilidades de los coordinadores claves y de los gerentes
- Proceso de comunicación que se debe seguir durante las emergencias
- Cómo interactuar con las autoridades e identificarlas a su llegada. Identificar en dónde se ubicarán las áreas de soporte
- Ubicación de áreas seguras o alternativas y las rutas para llegar a ellas para los empleados de Facilities y cómo identificarlos
- Instrucciones generales de Seguridad
- Protocolos para manejo de medios

## PLAN DE RECUPERACIÓN DE INCIDENTES

- Información de contacto (internos y externos)
- Información que ayude al gerente de emergencias en la toma de decisiones, identificando el curso de acción correcto
- Una lista de preguntas que hacer (Check list)
- Información del edificio, incluyendo planos, ubicación del panel eléctrico y de alarma contra incendios, ubicación de materiales peligrosos e inflamables, válvulas de cierre de gas, agua e interruptor eléctrico
- Cómo revisar y auditar todo lo anterior


APAFAM

# FACTORES QUE REQUIEREN ATENCIÓN DIRECTA DURANTE EMERGENCIAS

- Controlar accesos.
- Proteger la propiedad.
- Evacuación completa o parcial.
- Atención de emergencias médicas.
- Proveer seguridad.
- Coordinar actividades con las autoridades locales.
- Manejo de materiales o desechos peligrosos
- Comunicación a las partes interesadas.

# EVALUACIÓN Y DOCUMENTACIÓN DE DAÑOS

- El equipo de evaluación de daños requiere de expertos
- El equipo requiere:
  - Planos "as-built" que incluya renovaciones.
  - Fotografías de las instalaciones antes de los daños.
  - EPP o equipo de seguridad prescrito.
  - Dispositivos de ingeniería.
  - Registros de mantenimiento preventivo y correctivo.
  - Especificaciones de operación recomendadas por el fabricante.
  - Checklist de inspección y auditoria de maquinarias y equipos.
  - Otros equipos.

## PREGUNTAS INMEDIATAS DE EVALUACIÓN

- ¿Hubo pérdidas humanas?
- ¿Qué tan extenso fue el daño?
- ¿Se mantienen los servicios de utilidades?
- ¿Las instalaciones están creciendo o expandiéndose?
- ¿Hay riesgo inminente de explosión o caída?
- ¿Se deben evacuar las áreas circundantes?
- ¿El agua estancada puede ser un riesgo?
- ¿Los documentos y registros importantes de la organización están accesibles?
- ¿Se requiere de apoyo adicional?
- ¿Qué ocasionó la situación?

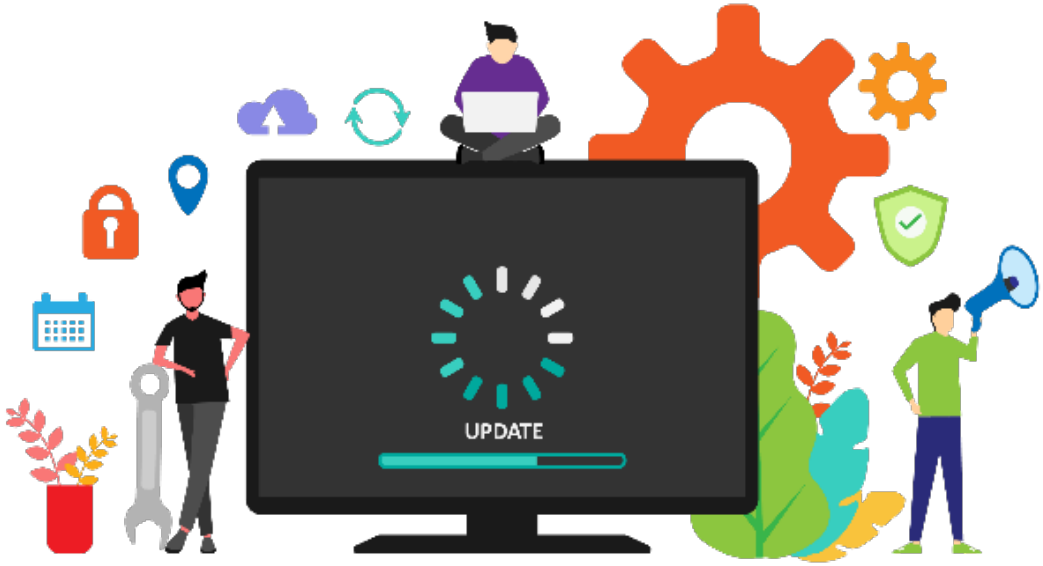
# PLAN DE COMUNICACIÓN DE EMERGENCIAS

**DEBE INCLUIR:**

- Un guion desarrollado para situaciones de emergencia y potencialmente emocionales.
- Hoja con detalles de la organización/facilidad y métodos de respuesta a emergencias.
- Anuncios a los ocupantes del edificio con información de expectativas/instrucciones de emergencias.
- Notificaciones a las familias de los empleados de lo ocurrido, a quién contactar, soporte y el plan que se está siguiendo.
- Comunica, para la tranquilidad de los clientes , sobre la preparación, respuesta y recuperación. Así como cómo les puede impactar la emergencia.


# IMPLEMENTANDO PLANES DE RECUPERACIÓN

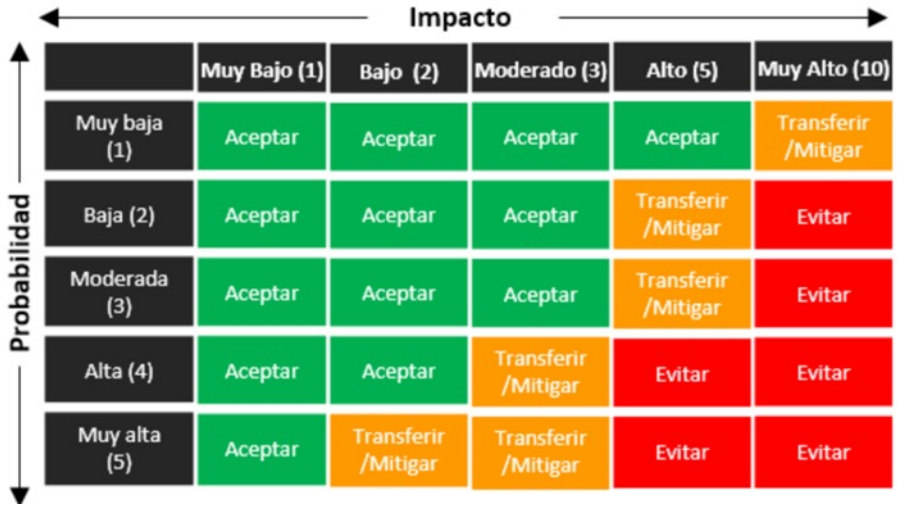
1. Notificar a la compañía aseguradora.
2. Coordinar los esfuerzos de bomberos, policía, inspectores u otras entidades oficiales
3. Prepararse para o conducir una evaluación de las condiciones del edificio (afectaciones)
4. Iniciar la creación de plan de recuperación de la instalación
5. Preparar para, coordinar y comunicar los resultados de evaluaciones (afectaciones)
6. Acceda al plan de continuidad del negocio para iniciar su ejecución.




7. Conducir un inventario de todos los equipos, insumos, partes y herramientas que se hayan dañado.
8. Reportar al personal de Facility y Property Management y a los contratistas que estén desarrollando tareas regulares
9. Agendar y coordinar las tareas de limpieza
10. Asegurar que los materiales peligroso y otros escombros se manejen siguiendo las regulaciones y ordenanzas de las regulaciones ambientales.
11. Identificar y catalogar todos los costos asociados al plan de recuperación
12. Facilitar la restauración de los sistemas y alarmas de seguridad humana, ambiental, seguridad física y de pánico
13. Coordinar la reparación y prueba de los sistemas de ventilación, eléctricos, de gas, sanitarios y de agua
14. Obtener aprobación por las entidades pertinentes para la puesta en marcho u operación.

Proyecto: Mantenimiento Aleros Exteriores (impermeabilización y pintura)


¿Quiénes van a identificar los riesgos? Líder del Proyecto y lider del Equipo de S&LP
¿Cuándo se llevará a cabo la identificación de los riesgos? En la etapa de Planificación.
¿Qué herramienta se utilizará para el análisis cualitativo de riesgos? Matriz de Riesgo
¿Cómo se priorizarán los riesgos? Seguridad Humana
¿Cuáles serán las estrategias a implementar para cada riesgo?
¿Con qué frecuencia se realizará el monitoreo de riesgos? Diariamente




MODERADO
Ingreso de visitantes a las areas restringidas
Moderado:
ALTO
Caídas de material de altura
Ingreso de visitantes a las areas restringidas


# NORMAS ISO ASOCIADAS A RIESGOS Y SEGURIDAD FÍSICA

- **ISO 3100. Gestión de Riesgos.** Enfoque en detección, el análisis y la solución de riesgos.
- **ISO 2700. Sistema de Gestión de Seguridad de la Información**. No es directamente el enfoque, pero incluye parte de seguridad física y del entorno, focalizado en prevenir el acceso físico no autorizado a la información y a las instalaciones de procesamiento de información de las empresas.
- **ISO 23234. Criterios y recomendaciones de seguridad para planificar la seguridad de edificios.** La norma define el proceso de diseño e implantación a seguir, los entregables a considerar y qué profesionales deben involucrarse.
- **ISO 22341. Diseño del entorno para la prevención del crimen**

# ¡MUCHAS GRACIAS!


**LinkedIn**
www.linkedin.com/in/AlfonsoAlizoR

**Correo electrónico**
aalizo@towncenter.com.pa
alfalizo@hotmail.com

**Teléfono**
Personal: +507 6882 4837
Corporativo: +507 6650 1739

**Desarrollado en el marco de la celebración del**

WORLDFMDAY
Haciendo Una Verdadera Diferencia
10 MAY 2023
A Global FM™ initiative

APAFAM
Asociación Panameña de Facility Management

Business Park Costa del Este,
Avenida de La Rotonda, Torre Sur
+507 6277 2281 | info@apafam.com.pa
www.apafam.com.pa